

What is claimed is:

- 1 1. A method comprising:
2 initiating an operation in a second portion of a
3 system if a value indicates that a first portion of the
4 system is in a trusted state.
- 1 2. The method of claim 1, wherein the operation
2 comprises an information update.
- 1 3. The method of claim 2, further comprising setting
2 a register containing the value using the first portion
3 before exiting the trusted state.
- 1 4. The method of claim 3, further comprising reading
2 the value using the second portion.
- 1 5. The method of claim 1, further comprising not
2 performing the operation if the value is not indicative of
3 the trusted state.
- 1 6. The method of claim 1, further comprising
2 initiating remediation if the value is not indicative of
3 the trusted state.
- 1 7. The method of claim 2, further comprising
2 receiving the information update via an air interface with

3 the second portion and providing the information update to
4 the first portion.

1 8. The method of claim 1, wherein the second portion
2 comprises a communications processor of a wireless device
3 and the first portion comprises an applications processor
4 of the wireless device.

1 9. A method comprising:
2 maintaining a hardware asset to indicate a trust state
3 of a first subsystem of a system.

1 10. The method of claim 9, further comprising
2 accessing the hardware asset using a second subsystem of
3 the system.

1 11. The method of claim 9, wherein the system
2 comprises a wireless device.

1 12. The method of claim 10, further comprising
2 updating digital content in the second subsystem if the
3 hardware asset indicates the trust state is valid.

1 13. The method of claim 10, further comprising
2 preventing updating the second subsystem if the hardware
3 asset does not indicate the trust state is valid.

1 14. The method of claim 13, further comprising
2 performing a remediation measure using the second subsystem
3 if the trust state is not valid.

1 15. The method of claim 13, further comprising
2 providing an indication to the first subsystem if an update
3 was attempted when the trust state was not valid.

1 16. The method of claim 9, further comprising setting
2 the hardware asset via the first subsystem before exiting a
3 trusted state, wherein the hardware asset comprises a one-
4 way register.

1 17. The method of claim 10, further comprising
2 determining if an update is trusted in the first subsystem
3 and transferring the update to the second subsystem if the
4 hardware asset indicates the trust state is valid.

1 18. An apparatus comprising:
2 a hardware asset to indicate a trust state of an
3 applications portion of the apparatus.

1 19. The apparatus of claim 18, wherein the hardware
2 asset is accessible by a communications portion of a
3 wireless device.

1 20. The apparatus of claim 19, wherein the
2 communications portion cannot modify a value of the
3 hardware asset.

1 21. The apparatus of claim 18, wherein the hardware
2 asset is coupled to receive a program signal if the trust
3 state of the applications portion is not valid.

1 22. The apparatus of claim 18, wherein the hardware
2 asset is coupled to receive a reset signal to initiate a
3 trusted state.

1 23. The apparatus of claim 18, wherein the hardware
2 asset comprises a one-way register.

1 24. A system comprising:
2 a hardware asset to indicate a trust state of an
3 applications portion of the system; and
4 a wireless interface coupled to the hardware asset.

1 25. The system of claim 24, wherein the hardware
2 asset is accessible by a communications portion of the
3 system, wherein the system comprises a wireless device.

1 26. The system of claim 24, wherein the hardware
2 asset comprises a one-way register.

1 27. The system of claim 24, wherein the wireless
2 interface comprises an antenna.

1 28. An article including a machine-accessible storage
2 medium containing instructions that if executed enable a
3 system to:

4 control a hardware asset of the system to indicate a
5 trust state of a first portion of the system.

1 29. The article of claim 28, further comprising
2 instructions that if executed enable the system to update a
3 second portion of the system if the hardware asset
4 indicates the trust state is valid.

1 30. The article of claim 28, further comprising
2 instructions that if executed enable the system to prevent
3 or discard an update to a second portion of the system if
4 the hardware asset indicates the trust state is not valid.

1 31. The article of claim 30, further comprising
2 instructions that if executed enable the second portion to
3 initiate a remediation operation if the hardware asset
4 indicates the trust state is not valid.

1 32. The article of claim 28, further comprising
2 instructions that if executed enable the system to perform
3 a secure operation in a second portion of the system if the
4 hardware asset indicates the trust state is valid.

1 33. The article of claim 28, further comprising
2 instructions that if executed enable the first portion to
3 vector into a trusted state before initiating a transfer
4 operation to a second portion of the system.

1 34. A method comprising:
2 accessing a value with a second portion of a system,
3 the value indicative of a trust state of a first portion of
4 the system.

1 35. The method of claim 34, further comprising
2 initiating an operation in the second portion if the value
3 is indicative of the trust state.

1 36. The method of claim 35, wherein the operation
2 comprises an information update.

1 37. The method of claim 34, wherein the first portion
2 comprises an applications portion of a wireless device and

3 the second portion comprises a communications portion of
4 the wireless device.